

Understanding Wireless LAN Routers

Contributed by Jim Geier
Tuesday, 20 March 2007

By definition, a router transfers packets between networks. The router chooses the next best link to send packets on in order to reach closer to the destination. Routers use Internet Protocol (IP) packet headers and routing tables, as well as internal protocols to determine the best path for each packet. Most routers connect a LAN (like the one in your home or office) to a WAN (like the cable system running your cable modem) by interfacing a broadband modem to the network within the enterprise, small office, or home.

A wireless LAN router adds a built-in access point function to a multi-port Ethernet router. This combines multiple Ethernet networks with wireless connections as well. A typical WLAN router includes four Ethernet ports, an 802.11 access point, and sometimes a parallel port so it can be a print server. This gives wireless users the same ability as wired users to send and receive packets over multiple networks. 802.11b, 802.11a, and 802.11b/a combo WLAN routers are now available from several vendors such as Netgear, D-Link and Actiontec. 802.11g routers are also starting to come on the market.

WLAN Routers vs. Access Points

There may be some confusion over the difference between WLAN routers and access points. The main thing to remember is that access points allow wireless clients access to a single network, while WLAN routers allow clients to browse a number of different networks. The router always takes the IP address into account to make decisions on how to forward (i.e., route) the packet; whereas, access points generally ignore the IP address and forward all packets.

In addition, WLAN routers implement the Network Address Translation (NAT) protocol that enables multiple network devices to share a single IP address generally provided by the Internet Service provider (ISP). WLAN routers also have the ability to provide port-based control, firewall management and Dynamic Host Configuration Protocol (DHCP) services for all devices. These functions make the WLAN router much more versatile than an access point.

Why use a WLAN router?

Consider using a WLAN router for the following reasons:

IP address sharing. WLAN routers offer strong benefits in the home and small office setting. For example, you can subscribe to a cable modem service that provides a single IP address through DHCP to the router, and the router then provides IP addresses via DHCP to clients on your local network. NAT then maps a particular client on the local network to the ISP-assigned IP address whenever that client needs to access the Internet. As a result, you need a router if you plan to have more than one networked devices on a local network sharing a single ISP-assigned address. Instead of having one box for the router and another box for the access point, a WLAN router provides both in the same box.

Connect multiple networks. WLAN routers are also ideal for wireless networks in public areas, especially if there are multiple networks that are accessible. For instance, a University may have a separate network in each of its buildings. Students sitting outside might want to gain access one or more of these networks and also surf the Internet. A WLAN router enables them to access everything through the wireless connection.

Improve network management. WLAN routers in an enterprise environment give network administrators an extra way to monitor and update their networks. In addition to being able to log on either locally or remotely via the wired network, they will be able to log on wirelessly and make any observations or changes.

Improve network performance. Because routers only send packets to specific, directed addresses, they do not forward the often numerous broadcast packets that are sent out by other devices. This results in an increase in throughput because of lower utilization on the network and less work needed by the router. This enables WLANs to operate much more effectively. The router, however, will offer more delay than an access point, but the impacts are generally unnoticeable.

Increase security. A strong advantage of WLAN routers is that they provide an added layer of security, both on the wired side and wireless side. The wired side is usually protected by a firewall and has extensive access control filters. These

filters can be set based on MAC (medium access control) address, IP address, URL, domain name, and even a set schedule that allows access only at certain times. If an unauthorized user tries to access the network, an e-mail alert is immediately sent to the network administrator. For supporting sensitive information, many WLAN routers support multiple and concurrent IPsec sessions, so users can more securely access networks through a range of virtual private network (VPN) clients. Most WLAN routers also implement wired equivalent privacy (WEP) encryption.

Configuring a WLAN Router

Most WLAN routers are easy to install and configure. Physically connecting the unit to a broadband modem or hub is made easier through clearly written instructions, labeled ports and illustrations.

When installing a WLAN router, consider the following:

Identify the IP address and domain server address for the WAN (broadband connection) side of the router. You will need to configure the router with these addresses. In some cases, the ISP provides these addresses through DHCP. In this case, you'll need to activate DHCP for the router's WAN port.

Define IP addresses for the local side of the router. In most cases, especially with wireless networks, DHCP is the best way to assign addresses to client devices on the local network (wireless and wired LAN side of the router). As a result, configure the router to assign these addresses via DHCP. Assign a starting and maximum number of addresses that you want DHCP to assign. Be sure to include all network devices. This includes potential PDAs and printers in addition to PCs and laptops that may access the network.

Configure 802.11 parameters on the access point. This includes the service set identifier (SSID), WEP, radio frequency channel, transmit power and other functions such as request-to-send / clear-to-send (RTS / CTS) and fragmentation. Be sure to set the SSID and administrative login user name / password to a non-default value to improve security. For single access point networks, you can probably use the default radio channel, but another channel might be needed to avoid conflicting with other nearby access points. In most cases, set the transmit power to the highest value (usually the default setting). Other settings will depend on application requirements.

A WLAN router is certainly a component to consider for any Wi-Fi deployments. It pulls together the routing and access point functions into a single component that is relatively easy to configure and manage. When deploying WLANs, however, also consider the use of bridges and repeaters.

Jim Geier is an independent consultant and founder of Wireless-Nets, Ltd (www.wireless-nets.com), a consulting firm assisting municipalities, enterprises, hospitals, airports, and equipment providers with the development and deployment of wireless networks.